GILBERTO M. GARCIA
Attorney At Law
25 East Spring Valley Avenue
Suite 330
Maywood, New Jersey 07607
Tel : (201) 328-7042
Fax : (201) 445-5855
gilberto13@me.com

Attorney For Plaintiff

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

FRANCESCO CORALLO — CIVIL ACTION

Plaintiff,

v.

BERKELEY RESEARCH GROUP, LLC
NSO GROUP TECHNOLOGIES LIMITED
and Q CYBER TECHNOLOGIES LIMITED — COMPLAINT

Defendants. — DEMAND FOR JURY TRIAL

PRELIMINARY STATEMENT

1. This is an action brought by the Plaintiff against the Defendants Berkeley Research Group, LLC ("Berkeley"), NSO Technologies Limited ("NSO") and Q Cyber Technologies ("Q Cyber"). Plaintiff seeks judgment in this Court against Defendants for relief permitted under 18 U.S.C. §1030 ("Computer Act"), 28

U.S.C. §1605(a)(5) the exception to the Foreign Entities Immunities Act, and common law violations of his invasion of privacy.

2. This action is also brought seeking a declaratory judgment that NSO violated plaintiff's privacy and must provide the information against defendant NSO to provide the list of its customers that hacked plaintiff's Apple accounts, including his iPhone and iCloud.

3. This action also seeks redress against the suspected foreign sovereignties, the Netherlands and Italy, that, on information and belief, acted as customers of NSO and conspired with NSO to intentionally hack plaintiff's Apple devices and systems and violated plaintiff's privacy with their spyware. The plaintiff provides sufficient facts herein that qualify, based on his information and belief, as sufficient facts forming his belief that he was hacked, and his privacy violated by the foreign sovereign entities. Furthermore, and more significant, the information alleged herein regarding the customers of NSO is all within the possession of NSO and the foreign sovereignties.

4. Plaintiff cannot be certain of which state-sponsored attacker hacked into his iPhone and iCloud account, using NSO hacking tools because defendants refused to disclose this information.

5. However, both Italy and the Netherlands, each on its own and jointly, have over the years subjected plaintiff to severe persecution and elicited on plaintiff's political views and his business interests. This persecution manifested in illegal and intrusive surveillance of plaintiff, his family, business associates and attorneys.

6. Plaintiff has been deliberately accused in and by the media of being associated with organized crime, and of all sorts of criminal activity, in an apparent attempt to discredit and defame plaintiff. Persecution led to prosecution, however, none of these public allegations have ever resulted in a conviction of plaintiff in a court-of-law.
7. Plaintiff had been incarcerated by the Netherlands authorities for months, in totally inadequate police holding cell, pending extradition to Italy, exceeding the maximum pretrial detention allowed by law by months and in excruciating circumstances.
8. The European Court on Human Rights has condemned the Netherlands for basic human rights violations and torture.
9. Plaintiff fears that this persecution and prosecution has now also taken the shape of illegal and extra-judiciary methods, causing immense stress and anxiety to him, his family, notably his American twin daughters, and close collaborators, but at the same time considers this current behavior as an unfortunate continuation of these countries' past behavior.
10. Plaintiff believes that this prosecution has also a political nature as plaintiff's principal business is with the Italian State, based on a non-exclusive State concession for the networking of and collection of taxes from gaming machines. Historically plaintiff had and continues to have various business interests in the small territory of Sint Maarten, a former island territory of the Kingdom of the Netherlands, but since October 2010 an autonomous country in said Kingdom.

11. Plaintiff believes that both his involvement in the Italian State concession business, as well as his presence in the closely knit Sint Maarten society have drawn the ire of the authorities of both countries, resulting in a more and more intense scrutiny of and attack against his person and business interests in both locations. The extent of scrutiny of Plaintiff can be demonstrated by the fact that on two occasions plaintiff's alleged influence on Sint Maarten's politics was discussed in the Dutch Parliament, while in Italy the government enacted 3 ad-personam laws in relation to the concession business, dubbed 'anti-Corallo laws'.
12. Plaintiff has denounced on several occasions to the Italian prosecutors, that the exact same behavior (although perfectly legal) his Italian business is prosecuted for was conducted by all the other (9) concessionaire companies. But no other company has ever been prosecuted (as firmly stated by the law), confirming Plaintiff's conviction that he has been singled out on a permanent basis.
13. Defendant NSO is a notorious hacker and has been described as a mercenary that has created a highly sophisticated cyber surveillance machinery that invite routine and flagrant abuse. It designed, developed, sold, delivered, deployed, operated, and maintained offensive and destructive malware and spyware products and services that have been used to target, attack, and harm apple users such as the plaintiff, and Whatsapp users such as the plaintiff. NSO has done this for its own commercial gain, enabling their customers to abuse those products and services to target individuals like the plaintiff and government officials, journalists, businesspeople like the plaintiff, activists, academics, and citizens all around the world. NSO is the operative that has caused the severe damage to many people

and organizations throughout the world, thus causing death and destruction of innocent people's lives with no conscience whatsoever and to date, with no repercussion for its evil and illegal conduct.

14. Defendant NSO Group was incorporated in Israel on January 25, 2010, as a limited liability company. Ex. 1. NSO Group had a marketing and sales arm in the United States called WestBridge Technologies, Inc. Between 2014 and February 2019, NSO Group obtainedfinancing from a San Francisco–based private equity firm, which ultimately purchased a controlling stake in NSO Group. In and around February 2019, NSO Group was reacquired by its founders and management. *Id.* NSO Group's annual report filed on February 28, 2019, listed Defendant Q Cyber as the only active director of NSO Group and its majority shareholder.

15. Defendant Q Cyber was incorporated in Israel on December 2, 2013, under the name L.E.G.D. Company Ltd. On May 29, 2016, L.E.G.D. Company Ltd. changed its name to Q Cyber. Until at least June 2019, NSO Group's website stated that NSO Group was "a Q Cyber Technologies company." Q Cyber's annual report filed on June 17, 2019, listed OSY Technologies S.A.R.L. as the only Q Cyber shareholder and active Director.

16. At all times material to this action, each Defendant was the agent, partner, alter ego, subsidiary, and/or coconspirator of and with the other Defendant, and the acts of each Defendant werein the scope of that relationship. In doing the acts and failing to act as alleged in this Complaint, each Defendant acted with the knowledge, permission, and consent of each other; and, each Defendant aided and abetted each other in their malicious activities.

17. These malicious activities have led to the United States government imposing sanctions against NSO. The US government confirms that defendants' product and services have enabled foreign governments to conduct transnational repression. Such practices threaten the rules' based international order.
18. This action seeks redress for defendants' multiple violations of federal law arising out of their egregious, deliberate, and concerted efforts to target and attack the plaintiff, an Apple customer, and a WhatsApp user.
19. The plaintiff's privacy and property were damaged through the dangerous malware and spyware that defendants develop, distribute to third parties, and use or assist in using others to cause serious harm to the plaintiff. Defendants perpetrated an attack on plaintiff's data stored on his device.
20. When plaintiff chose to purchase Apple devices and iCloud storage, he did so because he trusted Apple's reputation for being the best in class and security features, being recognized as the safest and most secure mobile device on the market.
21. On the other hand, NSO products are not ordinary consumer malware. NSO has no interest in serving up annoying pop-up ads or even spoofing your bank to siphon money from your checking account. NSO's products are far more insidious and often highly sophisticated. The product sold to sovereign governments that pay hundreds of millions of dollars is used to target and attack a tiny fraction of users with information of particular interest to its customers. The average consumer is not of interest to or attacked by NSO or its customers. Given

the unfair and unjust treatment of the plaintiff by some foreign sovereign entities, he is not considered an average consumer. Plaintiff was directly targeted, upon information and belief, by the foreign sovereignties of Italy and Netherlands. Unfortunately, despite his search and inquiries, plaintiff has been unable to discover the foreign entity that requested defendant NSO to hack his account and that is part of his injunctive relief request here.

22. NSO has admitted to the fact that its destructive products have led to violations of fundamental human rights. These human rights violations have been widely recognized and condemned by human rights groups and governments, including the US government. NSO provides ongoing technical support and other services to their clients by deploying its spyware against apple products and users like the plaintiff in this case.

23. In the specific case of plaintiff, on October 9, 2018, the European Court of Human Rights rendered an opinion and judgment against the government of the Netherlands for violating plaintiff's human rights. *https://laweuro.com/p=5176*

24. Further, for political reasons, the government of Italy has been on a campaign for over a decade to unjustly attack the plaintiff with prosecutions and false accusations for socio political and financial reasons intended to eliminate the plaintiff's influence as a businessman from the Italian economy.

25. Based on the preceding statements, there is no doubt that either the Netherlands or Italy, both customers of NSO have contracted its spyware to spy on the plaintiff. Plaintiff must know in factual and evidential detail the harm caused by the

hacking of his Apple products and the co-conspirators of defendant NSO. Currently, the requested information is only withing the possession of NSO.

26. NSO's malicious activity regarding the plaintiff have caused the plaintiff damages by allowing its customers, in this case, upon information and belief, the countries of Netherlands and Italy, to hack into plaintiff's Apple product such as his iPhone, iCloud and his WhatsApp account. NSO's malicious products and services have also required the plaintiff to devote many hours to investigate the attack. Such investigation is continuing.

27. The difficulty presented by the conduct of the defendants creates a challenge for the plaintiff. Plaintiff is encountering difficulties in finding out the extent of his damage and NSO's co-conspirators because these defendants operate with impunity by hiding behind their unnamed customers, thus making it extremely difficult for those harmed such as the plaintiff to know the source that has caused the invasion of their privacy and the taking of significantly protected information regarding his life and his business. All will agree that it is outright disgusting to feel that unknown entities, some of them antagonistic and adversarial to the victim of the hack, have access to the victim's most private thoughts and property records. That is exactly what these defendants do in conspiracy and in business together with foreign sovereigns.

28. The NSO defendants are private companies and not sovereigns notwithstanding their former arguments in federal courts. Furthermore, and as significant, the foreign sovereignties suspected upon information and belief to have contracted with defendant NSO, Italy and the Netherlands, are not entitled to sovereign

immunity, nor do they enjoy any other immunity for their unlawful commercial and tortious conduct in relation to the hacking of plaintiff's Apple and WhatsApp accounts.

29. Defendant NSO's malicious and harmful activities, together with its customers, brought them well within the long arm of the law and the jurisdiction of this Court, which has the authority to hold them to account for their violations of U.S. federal laws and for the damages they have inflicted on the plaintiff.

30. In the case at hand both the Italian government and the Netherlands' government have engaged in a multi-year campaign designed to destroy the reputation and the well-being of the plaintiff, a businessman whose reputation has been intentionally tarnished by these two governments.

PARTIES

31. Plaintiff, Francesco Corallo is a native of Italy and a citizen of the Netherlands, who resides in Saint Maarten. He owns an iPhone and subscribes to iCloud and WhatsApp.

32. Defendant NSO was at all relevant times herein an Israeli limited liability company incorporated on January 25, 2010, and, on information and belief a subsidiary of defendant Q Cyber. NSO designs highly invasive and illegal spyware, which it sells, distributes, operates, maintains, and services for third parties around the globe, including the sovereignties of Italy and Netherlands.

33. Defendant Q Cyber was incorporated in Israel, on December 2, 2013, under the name L.E.G.D. Company Ltd. On my 29, 2016, L.E.G.D. Company Ltd. Changed its name to Q Cyber. NSO has described itself as a Q Cyber subsidiary.

34. Defendant Berkeley Research Group, LLC ("BRG"), is a U.S. consulting firm that now manages Q Cyber and NSO. BRG has offices at 250 Pehle Avenue, Suite 301, in Saddle Brook, New Jersey.

35. Italy is a foreign sovereign state that, according to reports issued by third parties, engaged defendant NSO to purchase the Pegasus and FORCEDENTRY to, among other things, spy on the plaintiff. Italy has an interest to spy on the plaintiff because for years it has been attempting to affect the plaintiff's interests in his business in Italy. By the conduct of hacking into plaintiff's Apple devices as described further, the foreign sovereignty of Italy cannot claim indemnity under 28 U.S.C. §1605(a)(5), the exception to the Foreign Entities Immunities Act.

36. Netherlands is a foreign sovereign state that, according to reports issued by third parties, engaged the NSO defendants to purchase the Pegasus and FORCEDENTRY to spy on the plaintiff. Netherlands has an interest to spy on the plaintiff because it is resentful for the plaintiff having obtained a judgment in the European Human Rights Court declaring the Netherlands in violation of plaintiff's human rights in 2018. By the conduct of hacking into plaintiff's Apple devices as described further, the foreign sovereignty of Netherlands cannot claim indemnity under 28 U.S.C. §1605(a)(5), the exception to the Foreign Entities Immunities Act.

37. The 9th Circuit has already held that the NSO defendants are not sovereigns and thus, not entitled to immunity, *WhatsApp, Inc. v. NSO Technologies Ltd., No. 20-16408 (9th Cir. Nov. 8, 2021).*

38. Against the foreign sovereignty of the Netherlands, the plaintiff pleads facts alleged upon information and belief and the facts pled are peculiarly within the possession and control of the defendants. Nevertheless, plaintiff's belief is based on information that makes the inference of the alleged culpability plausible. *Arista Records, LLC v. Doe 3, 604 F.3d 110 (2d Cir 2010).*

JURISDICTION

39. Jurisdiction is properly laid in this Court pursuant to 28 U.S.C. § 1331, and §1332.

40. The amount in controversy exceeds the sum or value of $75,000.00, exclusive of interests and costs and there is complete diversity between plaintiff and all the defendants. The Court has also federal jurisdiction over the federal causes of action alleged in this Complaint.

41. Venue is proper pursuant to 28 U.S.C. § 1391(b)(3) and (c)(3).

FACTS COMMON TO ALL CAUSES OF ACTION

42. On or about November 23, 2021, the plaintiff received notification from Apple advising him that his phone and his iCloud accounts had been hacked.

43. The official notice came from threat-notifications@apple.com, at 5:05 PM and it was sent to plaintiff's iCloud email.

44. The subject of the email was "Alert: State-sponsored attackers may be targeting your iPhone."

45. It advised that based on Apple's belief, plaintiff was being targeted by state-sponsored attackers who were trying to remotely compromise the iPhone associated with plaintiff's Apple ID.

46. The message further advised that the "attackers are likely targeting you individually because of who you are and what you do." The plaintiff is a businessman who has experienced harsh and unjust treatment from the sovereignties of Italy and Netherlands and that is the reason why his iPhone and iCloud account was hacked.

47. The plaintiff is a businessman. He owns casinos in St. Maarten and the Dominican Republic, and a business related to legal gambling collection and management of funds in Italy. He is a national of the Netherlands and native of Italy. He resides in Saint Maarten. His political enemies in Italy and the Netherlands have waged a campaign for more than a decade replete with unsubstantiated misinformation and false allegations, including criminal charges, all to destroy his reputation.

48. The message from Apple further stated, "If your device is compromised by a state-sponsored attacker, they may be able to remotely access your sensitive data, communications, or even the camera and microphone." Upon information and belief since the information is within the control of NSO and the foreign sovereignties, defendant NSO directly accessed or aided and abetted the sovereignties of Italy and Netherlands with the proper hacking device to access plaintiff's Apple account with the systems described herein.

49. The message further states "While it's possible that this is a false alarm, please take this warning seriously," The alarm was not false. See *WhatsApp v. NSO Group, et. al. No 4:19-cv-7123 (N.D. Cal. Oct. 29, 2019); Apple, Inc. v. NSO Group Technologies Limited, et. al., No.5:21-cv-09078 (N.D. Cal. Nov. 23, 2021).*
50. Apple recommended that plaintiff update his iPhone to the latest software version, which the plaintiff did.
51. Apple also recommended that plaintiff enlist expert help such as the rapid response at the nonprofit Access Now, at accessnow.org/help. Plaintiff read the article.
52. Apple further recommended that plaintiff be cautious with all links he received. Plaintiff followed the advice.
53. Plaintiff also signed out of all messaging and cloud services.
54. Plaintiff also restored his device to factory settings and purchased a new iPhone.
55. Plaintiff engaged his employees to investigate the technical aspects of the invasion of his iPhone and his iCloud account.
56. The Plaintiff retained counsel to seek information regarding the hacking of his Apple devices.
57. The Apple iPhone contains a security feature called Blast Door. These feature takes incoming messages and unpacks and processes their contents inside a secure and isolated environment where malicious code hidden inside a message cannot interact with or harm the iPhone's operating system or even gain access to an Apple user's data. Notwithstanding all these protections, the defendant NSO discovered ways to bypass Blast Door's initial implementation.

58. Apple also provides multiple layers of protection to help ensure that the third-party apps that run on its operating systems are free of known malware and are not tampered with. These hardware innovations are continuously enforced.

59. Despite all these protections for Apple consumers, defendant NSO developed and deployed a highly invasive spyware known collectively as "Pegasus," which NSO describes as a cyber intelligence solution that enables its clients, like the country of the Netherlands to remotely extract valuable intelligence from virtually any mobile device.

60. According to NSO, Pegasus is installed remotely on a device through fraud or deception and without its owner's consent. The harm that Pegasus can cause is its recording using a device's microphone and camera, track the phone's location data, and collect emails, text messages, browsing history, and a host of other information accessible through the device. These allegations were first made in the matter of *WhatsApp v. NSO Group, et. al. No 4:19-cv-7123 (N.D. Cal. Oct. 29, 2019) Dkt 1-1 at 44.*

61. The Washington Post reported in July 2021 that defendant NSO and its clients, including the Netherlands, have deployed Pegasus to attack and surveil scores of individuals, including the plaintiff, journalists, human rights activists, government officials, and dissidents across more than 50 countries. *Dana Priest, et. al. Private Israeli spyware used to hack cellphones of journalists, activists worldwide, Washington Post – July 18, 2021. https://tinyurl.com /h5pw3uz.*

62. Upon information and belief, NSO and the sovereignties of the Netherlands and Italy deployed the Pegasus to target the Apple device of the plaintiff without his

consent. The Defendants planned specific attacks on the plaintiff's Apple devises, working with the sovereignty of the Netherlands to ensure that the spyware payload was delivered and operated to its maximum effect.

63. On information and belief, from at least February until September of 2021, the NSO deployed its Pegasus spyware through an exploit that Citizen Lab named FORCEDENTRY.

64. Citizen Lab is a most needed security research organization based at the Munk School of Global Affairs & Public Policy, University of Toronto, that investigates digital espionage against civil society and protects citizens of the world from being exploited by spyware attacks like the ones designed here by the defendants.

65. The FORCEDENTRY is known as a "zero-click" exploit, meaning that it allows the violator like the defendants here to hack into the victim's device without any action or awareness by the victim. FORCEDENTRY was identified in March of 2021.

66. On March 17, 2021, Ronald Van Raak stated to the press that he had special documents that cover what he libelously called the gambling mafia of the Antilles, referring in a defamatory manner to the legal operation of plaintiff's gambling casinos in St. Maarten. He further stated that the documents had come into his possession in one way or another and that a member of Parliament never has to disclose his source, therefore, anyone can share anything with a member of the Netherlands Parliament. The source of Van Raak's information, which he discussed publicly, is only in his possession and he obtained the information from this source during his tenor as a member of the Dutch Parliament.

https://www.volkskrant.nl/.nieuws-achtergond/.meer-onderzoek-doen-minder-naartalkshows-adviseert-ronald-van-raak-na-18-jaar-tweede-kamer~b4bdc7f9/.

67. Ronald Van Raak stated that the information he was gathering had been shared by and with the Italian Secret Service. Upon information and belief NSO and the foreign sovereignty of the Netherlands is a customer of NSO. Plaintiff seeks that NSO provide the plaintiff with the information it shared with the Netherlands.

68. On information and belief, the defendants herein were able to implement the FORCEDENTRY and Pegasus to spy on the plaintiff and thousands of other Apple users throughout the world by creating more than one hundred Apple IDs using Apple's systems to be used in their deployment of FORCEDENTRY. This was all done using Apple servers in the United States. *Apple, Inc. v. NSO Group Technologies Limited, et. al., No.5:21-cv-09078 (N.D. Cal. Nov. 23, 2021).*

69. According to cybersecurity research, news reports and the *Apple and WhatsApp v. NSO* litigation, following the delivery of Pegasus to an Apple device like the one plaintiff used, the spyware program would begin transmitting personal data to a command-and-control server operated by NSO and the sovereignties named as defendants in this matter. Other than physical torture, there can be nothing more damaging to one's self-respect and integrity than to know the harm and internal pain from a violation of one's most private information, including communications with others that are intended and should remain private. The plaintiff has been violated in way far more significant than the human rights violations in which the foreign sovereignty of Netherlands engaged.

70. On information and belief, NSO provided consulting and expert services to the foreign sovereignties of Italy and the Netherlands and assisted them with their deployment and use of Pegasus and participated in their attacks on the plaintiff's Apple device.

71. Upon information and belief, the NSO defendants' actions are apparently highly lucrative. NSO and its parent companies have reported revenue and earnings in the hundreds of millions of dollars. Like a company that engages in lies and illegal acts, NSO is now stating that it is in the brink of bankruptcy. Upon information and belief, NSO's representations are not to be believed. But this lawsuit, more than any kind of damages that the plaintiff could obtain in compensation for the hacking of his Apple accounts, seeks the identity of those parties who blatantly violated the greatest asset of human rights: the sacredness of privacy and the freedom to be an speak and act without being spied upon for no reason, except retaliation and the evil intent to cause harm without any basis.

72. Defendants' injurious actions have included all the misconduct described in the foregoing paragraphs, which are incorporated by reference herein, including but not limited to the development, deployment, maintenance, servicing, operation and other use of Pegasus and other spyware, malware and hacking devices to target, attack, exploit and cause harm to the plaintiff.

73. These actions have injured, harmed, and have caused damages to the plaintiff by forcing it to incur costs and to devote personnel, resources, and time to attempt to identify and investigate the attacks and exploits.

74. These damages caused by the defendants are significant and are in excess of $75,000.00 and in an amount to be proven at trial.

COUNT ONE

Computer Fraud Act Violations 18 U.S.C. §1030

75. Plaintiff repeats and realleges each and every allegation contained above as even fully set forth herein.

76. Plaintiff is an Apple user. His devices are his subscriptions to Apple iPhone device and iCloud. His iPhone is a "computer" as described by 18 U.S.C. §1030(e)(1).

77. Plaintiff's iPhone is a "protected computer" as defined by 18 U.S.C. §1030(e)(2)(B) because is "used in or affecting interstate commerce or communications in the United States.

78. Defendant NSO and the "foreign sovereign entities" Italy and Netherlands violated and attempted to violate and violated 18 U.S.C. § 1030(a)(2) because they intentionally accessed and attempted to access the iOS operating system in plaintiff's iPhone and his iCloud without authorization and, on information and belief, obtained information from his iPhone and iCloud.

79. Defendant NSO and its customers foreign sovereign entities violated 18 U.S.C. § 1030(a)(4) because they are knowingly and with the intent to defraud accessed the operating system on plaintiff's iPhone without authorization using information from the Apple servers and then installed highly invasive spyware on the plaintiff's iPhone and by means of such conduct furthered the intended fraud and

obtained and obtained information about the plaintiff illegally. This access was without authorization from the plaintiff or from Apple.

80. As a result of the fraud defendants NSO and the foreign sovereign entities obtained something of extreme value: financial and confidential and privileged communications between the plaintiff and others, including his close business associates and his attorneys.

81. Defendant NSO's and its co-conspirator foreign sovereign entities' actions caused the plaintiff to incur a loss as defined by 18 U.S.C. §1030(e)(11), in an amount of $5,000.00 during a one-year period, including the expenditure of resources to investigate and remediate defendants' illegal conduct. Plaintiff is entitled to compensatory damages in an amount to be proven at trial, as well as injunctive relief or other equitable relief in accordance with 18 U.S.C. §1030(g).

82. Defendant NSO and the foreign sovereign entities violated 18 U.S.C. § 1030(a)(5)(A) because they knowingly caused the transmission of a program, information, code, and/or command, specifically the commands needed to carry out the exploits described above, as well as Pegasus spyware itself, to Apple's servers, and as a result of such conduct intentionally caused damage without authorization to the operating system in plaintiff's Apple devices, including by installing the Pegasus spyware.

83. Defendant NSO and its co-conspirators foreign sovereignties violated 18 U.S.C. §1030(a)(5)(B) because they intentionally accessed plaintiff's Apple device without authorization and as a result of such conduct, recklessly caused damage to

the operating system on plaintiff's Apple device, including by installing the Pegasus spyware.

84. Defendant NSO and its co-conspirators foreign sovereignties violated 18 U.S.C. §1030(a)(5)(C) because they intentionally accessed plaintiff's Apple device without authorization and as a result of such conduct, recklessly caused damage to the operating system on plaintiff's Apple device, including by installing the Pegasus spyware.

85. Defendant NSO and its co-conspirators foreign sovereignties violated 18 U.S.C. §1030(b) by conspiring and attempting to commit the violations alleged in the preceding paragraphs.

COUNT TWO

Invasion Of Privacy

86. Plaintiff repeats and realleges each and every allegation contained above as even fully set forth herein.

87. Defendant NSO and its co-conspirators foreign sovereignties engaged in conduct that was not consented to by the plaintiff.

88. Defendant NSO and its co-conspirators foreign sovereignties caused a harm to the plaintiff with the acts described herein, which constitute an intentional invasion of plaintiff's rights to privacy.

89. The invasion, as described herein, was concrete and particularized; actual and imminent, not conjectural or hypothetical.

90. The injury arising from the acts complained of herein, has deeply affected the plaintiff in a personal and individual way and plaintiff does not have to show any

pecuniary harm at this point considering that invasion of privacy in and of itself constitutes an intentional tort on the part of NSO and its co-conspirators foreign sovereignties as described herein.

91. Defendant NSO and its co-conspirators foreign sovereignties intentionally intercepted the contents of plaintiff's electronic communications using a device in violation of the Wiretap Act, 18 U.S.C. §2511(2)(d) since NSO and its co-conspirators foreign sovereignties were not parties to the conversation and plaintiff would have never given consent to the interceptions.

92. Defendant NSO and its co-conspirators foreign sovereignties also harmed the plaintiff with their invasion of privacy by their violations of the Computer Fraud Act as alleged in COUNT ONE of this Complaint.

COUNT THREE

Foreign Sovereign Immunity Exceptions Pursuant To 28 U.S.C. §1605(a)(5)

93. Plaintiff repeats and realleges each and every allegation contained above as even fully set forth herein.

94. The foreign sovereign entities of Italy and the Netherlands, by, upon information and belief, having engaged in the conduct described herein, are not subject to the immunities afforded sovereign entities pursuant to 28 U.S.C. §1602.

95. In fact, foreign states shall not be immune for the jurisdictions of the courts of the United States in actions where money damages are sought against such foreign state for personal injury, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state as described in all the allegations in this Complaint.

96. The foreign sovereign states of the Netherlands and Italy engaged in the invasion of plaintiff's privacy and the hacking of plaintiff's Apple devices and conspired with NSO to engage in all these acts. As a result, they cannot claim immunity and must answer to the allegations herein.

COUNT FOUR

Trespass To Chattels

97. Plaintiff repeats and realleges each and every allegation contained above as even fully set forth herein.

98. At all times mentioned in this Complaint, plaintiff had legal title to and actual possession of his device.

99. Defendants intentionally and without authorization interfered with plaintiff's possessory interest in his device, including by accessing and using Apple and WhatsApp servers to transmit its malicious code for the purpose of unlawfully compromising the plaintiff's targeted devices, all without authorization from plaintiff's.

100. Defendants' actions caused Plaintiffs to incur losses and other economic damages, including, among other things, the expenditure of resources to investigate and remediate Defendants'conduct, damage to Plaintiffs' reputation, and damage to the relationships and goodwill between Plaintiffs and their users and potential users. Plaintiffs have been damaged in an amount to be provenat trial, and in excess of $75,000.

DEMAND FOR JURY TRIAL

Plaintiff demands trial by jury.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff FRANCESCO CORALLO, request judgment against Defendants as follows:

1. That the Court enter declaratory judgment against Defendants that Defendants have:

   a. Violated the Computer Fraud and Abuse Act, in violation of 18 U.S.C. § 1030;

   b. Are not subjects to the Indemnities of The Foreign Sovereignties Act, 28 U.S.C. §1605(a)(5).

   c. Invaded Plaintiff's Privacy;

   d. Wrongfully trespassed on Plaintiffs' property by hacking his devices.

   e. That Defendant NSO must provide to the Plaintiff all customers that used Plaintiff's device to obtain his information.

   f. That Defendant NSO must provide the entities that paid it, and how much, to hack Plaintiff's devices.

2. That the Court enter a permanent injunction enjoining and restraining Defendants and their agents, servants, employees, successors, and assigns, and all other persons acting in concert and conspiracy with any of them or who are affiliated with Defendants from:

   a. Accessing or attempting to access Plaintiff's Apple devices and WhatsApp account;

3. That Plaintiff be awarded damages, including, but not limited to, compensatory, statutory, and punitive damages, as permitted by law and in such

amounts to be provenat trial.

4. That Plaintiff be awarded his reasonable costs, including reasonable attorneys' fees.

5. A permanent injunction requiring Defendants to identify the location of any and all information obtained from Plaintiff's devices, including but not limited to Plaintiff's iPhone, iCloud and WhatsApp account, and to delete all such information, and to identify any and all entities with who Defendants shared such information.

6. Any other relief as this Court deems just and proper.

/s/ Gilberto Garcia

_____

GILBERTO M. GARCIA
ATTORNEY FOR PLAINTIFF FRANCESCO CORALLO
25 East Spring Valley Avenue
Maywood, New Jersey 07607
Gilberto13@me.com
201-3287042